Kick-off Meeting:
Secure Communication in the Quantum Era

Discussion about Milestone 1A – Choice of security model

Rainer Steinwandt (Florida Atlantic University)

Basic Goal: Authenticated Group Key Establishment

- **What kind of authentication tool do we have in mind?**
  - (Post-quantum) signatures
  - Passwords
  - …

  → Signatures might offer easiest starting point; depending on protocol design, temporary assumptions could be of interest to alleviate concerns about message size

- **Should we consider "one-piece" design or step-wise design with compiler(s)?**
  - Natural starting point: 2-party KEMs submitted for NIST standardization
  - Even with a compiler, target solution with no more than 3-4 rounds for any number of participants

- **Initial design: ignore implementation-level attacks**
  - (Quantitative) security guarantees based on protocol-level attacks
  - Should facilitate reuse of existing results in the cryptographic literature

Considerations for Choosing the Security Model and Protocol Design

- **Goal is a protocol that can actually be implemented**
  - Accept idealizing assumptions, if standard assumption is likely to cause efficiency or/and implementation overhead
  - Security analysis should facilitate quantitative bounds – purely asymptotic analysis is less helpful

- **Cryptographic primitives should allow confidence in parameter choices**
  - primitive description likely generic (e.g., KEM, signature), but tailor protocol design towards use with lattices or/and codes.
    → consult with "resident experts" on state-of-the-art
  - Upcoming NIST-funded project at FAU, which documents analysis status of submissions to NIST's post-quantum standardization effort, will likely be a useful resource for us

- **"Oracle-based" model seems plausible choice**
  - commonly used for protocols in the literature and existing compilers
  - substantial expertise in the project team
  - quite flexible, one could potentially consider extension to reflect some implementation-level attacks

Impact of Quantum Information Processing on Model?

- **The obvious: our assumptions and parameters must make sense**
  - Assume scalable quantum computing available to adversary.
  - *Noisy Intermediate-Scale Quantum Computing* seems too weak of a model and unnecessarily restrictive for this project.

- **Possibilities we may want to ignore for now, as the assumptions seem too strong**
  - running protocols in superposition
  - superposition queries on key-dependent primitives
  - … and probably we should also not consider QKD as a primitive, so that we can focus entirely on classical protocol solutions and platforms?

- **What we may want to consider: quantum random oracle model (QROM)**
  - It seems reasonable to allow an adversary to experiment with a hash function in a controlled environment.
  - We need to be aware of QROM analyses of submissions for NIST post-quantum standardization.

Advanced Goal: Protect Implementation

- **Needed:** input from Malta partner on the type of guarantees that can be verified (efficiently) during runtime
  - will likely depend on implementation platform we are using
  - orthogonal to cryptographic guarantees established on protocol level, protection mechanisms should not interfere with protocol level, i.e., they should not jeopardize the higher-level security proof/reduction
  - if runtime problem is detected, how should/can we react?

Possibly a good topic for discussion for today?

- **Expected implementation items of concern**: provoked misbehavior in
  - pseudo-random number generation
  - signature verification
  - possibly signature generation